UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/811,823	03/20/2001	Edward Rodriguez	003918-025	9310

21839 7590 11/28/2007

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
LE, NANCY LOAN T	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
11/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
debra.hawkins@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	09/811,823	RODRIGUEZ ET AL.	
	Examiner	Art Unit	
	NANCY T. LE	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

Applicant's amendment filed on 19 October 2006 is acknowledged.

This paper is assigned Paper No. 20071015 by the Examiner.

Status of Claims

Claims 1-47 have been examined and remain pending.

Response to Arguments

Applicant's arguments filed 10/19/2006 have been fully considered but they are not persuasive. Applicant contends that the prior art reference Bayer et al. (U.S. 6,311,190 B1) do not teach the features of "*transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer; and transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter*". The Office respectfully disagrees as the Bayer reference indeed teaches "*transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer*" (Abstract, col. 29 line 64 – col. 30 line 8); *and "transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter*" (col. 30 lines 8-13).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. §103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-19, 23-40 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,250,548 B1 to McClure et al. in view of U.S. Patent No. 6,311,190 B1 to Bayer et al..

As per **claim 1**, McClure et al. disclose a method for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising the steps of:

- transmitting a blank electronic ballot, upon request by the registered voter at a second computer, from the computer database that resides on the transaction repository server, via the transaction mediator, to the second computer (*i.e., The voter returns to the jurisdiction's home page and selects the cast ballot option – col. 37, lines 4-5; The ballot style information supplied by the issue number allows the Internet voting software to retrieve the ballot style data {i.e., blank electronic ballot} from the database and display it on the screen for the voter – col. 37, lines 17-20*); and
- transmitting a voted electronic ballot from the second computer, via the transaction mediator, to the computer database that resides on the transaction repository server (*i.e., Once the voter activates the cast ballot button, the executable code stored previously encrypts the resulting data using information from the identification file and transmits the data packet {i.e., including the voted ballot} to the Internet software host -- col. 37, lines 26-29; After verifying valid switch positions, ... , the Internet software randomly saves the ballot image in a secure database ... -- col. 37, lines 32-36).*

McClure et al., do not expressly disclose such a method comprising the steps of:

- transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer;
- transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter;

Bayer et al., however, suggest a method for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising the steps of:

- transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer *(i.e., "**The system** allows voters, or other registrants, to register at one of the registration campaigns at the registration site, which may be linked to a voting campaign, **by constructing a registration questionnaire based on the registration information stored in the database, and sending the questionnaire in a registration form page in the voter's language to the voter** to complete and return to the network server for storage of the voter's registration data" – Abstract: the last sentence, col. 29 line 64 – col. 30 line 8)*;
- transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter (*i.e., "**The system** allows voters, or other registrants, to register at one of the registration campaigns at the registration site, which may be linked to a voting campaign, by constructing a registration questionnaire based on the registration information stored in the database, and sending the questionnaire in a registration form page in the voter's language to the **voter to complete and return to the network server for storage of the voter's registration data**" – Abstract: the last sentence, col. 30 lines 8-13)*;

to establish a registered voter over the network/Internet.

Therefore, it would have been obvious to and motivated by an ordinary skill in the art at the time the invention was made to modify a method for completing and submitting an electronic voter registration form and an electronic ballot over a network as disclosed by McClure et al. to include "***transmitting a blank electronic registration form, upon request at a first computer, via a transaction mediator, to the first computer; transmitting registration information from the first computer, via the transaction mediator, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter***" as suggested by Bayer et al. to establish a registered voter over the network.

As per **claim 2**, McClure et al. disclose the method of claim 1, comprising:

- establishing at least one computer database on the transaction repository server that contains information associated with at least one of a voter registration status of a citizen and an electronic ballot status (i.e., *the voter registration database – col. 9, lines 29-33, the tallying and reports databases – col. 9, lines 47-49, all of which, of course, reside on servers*);
- requesting a status at the first computer from the transaction repository server (*i.e., once the voter completes the Internet vote request and the jurisdiction is notified, through their home page, that the request has been made – col. 36, lines 40-42, it is understood that the voter is awaiting/requesting a status of the registration*);
- determining a status message in response to the step of requesting by examining the at least one computer database (*i.e., Electronic officials verify the information supplied by the voter and approve the assignment of an "issue number" for the voter – col. 36, lines 59-61*); and
- transmitting the status message from the transaction repository server to the first computer (*i.e., The issue number {understood as the status} is electronically sent to the voter via the Internet to the address supplied by the voter and defines the proper ballot style for the voter – col. 36, lines 61-63*).

As per **claims 3, 22, and 47**, McClure et al. disclose the method and system of claims 2, 20, and 46, respectively, wherein the voter registration status of the citizen and the electronic ballot status are verified (*i.e., A valid issue number is required to gain access to the cast ballot option ... Given a valid issue number, the identification file {contains voter's identification information} is verified as* ***legitimate/eligible/legal/valid****, and the voter gains access to the cast ballot selection – col. 37, lines 5-15; After verifying valid switch positions {which are equivalent to the voter's responses}, as indicated for the voter's ballot style, the Internet software randomly saves the ballot image in a secure database ... -- col. 37, lines 32-36*).

As per **claims 4 and 44**, McClure et al. disclose the method/system of claims 1 and 41, respectively, wherein the network includes:

- an encrypted communication channel between at least one of the first and second computer and the transaction mediator, and an encrypted communication channel between the transaction mediator and the transaction repository server (*i.e., The standard communication protocols employed provide further protection and include Secure Sockets Layer (SSL) protocol {is cryptographic protocols which provide secure communications on the Internet – Wikipedia Encyclopedia} - a common feature in popular Internet access software/browsers, and Secure Multi-purpose Internet Mail {S/MINE} – col. 35, lines 52-67; col. 36, lines 1-9).*

As per **claims 5 and 45**, McClure et al. disclose the method and system of claims 1 and 41, respectively, wherein the registration information includes at least one descriptive element associated with a citizen (*i.e., ... the voter may be required to provide additional information such as sworn statements, driver's license, or birth certificate – col. 36, lines 24-27*).

As per **claims 6, 27, and 36**, McClure et al. disclose the method of claims 1, 23, and 32, respectively, wherein the step of transmitting registration information comprises:

- entering the registration information (McClure i.e., The voter completes the Internet vote request/registration form – col. 36, line 40); and
- digitally signing the registration information using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of a citizen, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the registration information *(i.e., The software provides a "firewall" function, encryption/decryption, digital signing, and support of* secure communication protocols – col. 35, lines 62-64. ... The *encryption/decryption and digital signature capability is used to encrypt data prior to transmission and decrypt received data. ... The digital signature capability is used to authenticate data that is both transmitted and received – col. 36, lines 1-6*).

As per **claims 7 and 14**, the method of claims 6 and 13, respectively, wherein the step of transmitting registration information comprises:

- erasing from the first computer information associated with the registration information once the registration information has been transmitted (*i.e., The voter's PIN would be required to access {i.e., log in to} the voting option of the Web page, ... , and submits a request/registration to vote – col. 36, lines 29-33. This implies that once the voting registration information has been transmitted to the jurisdiction, the voter would log-off the web site; thus, automatically erasing/clearing such information from his/her computer screen*).

As per **claims 8 and 15**, McClure disclose a method of claims 6 and 13, respectively, wherein the step of transmitting registration information comprises:

- verifying the digital signature using the public key of the public-private key pair (*by Digital Signature Standard, a public-key cryptographic standard issued in 1994 by the United States Nat'l Institute of Standards and Technology {NIST} to authenticate electronic documents. The DSS uses a Digital Signature Algorithm {DSA} to generate and verify digital signatures based on a public key, which is not secret, and a private key, which is known or held only by the person generating the signature. A digital signature serves to authenticate both the identity of the signer and the integrity of the transmitted information – Microsoft Computer Dictionary, fifth edition*).

As per **claims 9, 28 and 37**, McClure et al. disclose the method of claims 6, 27 and 36, respectively, wherein the public-private key pair and the cryptographic identification can be used by the citizen with respect to a plurality of electronic transactions (see citation given in claim 8 above).

As per **claim 10**, McClure et al. disclose the method of claim 1, wherein the step of transmitting registration information comprises:

- approving or denying a voting registration request at the computer database based on the registration information of a citizen (*i.e., Election officials verify the information supplied*

by the voter and approve the assignment of an 'issue number' {for the voting registration request} for the voter – col. 36, lines 59-61).

As per **claims 11, 24 and 34**, McClure et al. disclose the method of claims 1, 23, and 33, respectively, wherein the second computer is the first computer since registration and voting computers are client computers, thus are the same (understood).

As per **claims 12, 29 and 38**, McClure et al. disclose the method of claims 1, 26 and 33, respectively, wherein the step of transmitting a blank electronic ballot comprises:

- digitally signing the blank electronic ballot using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of an operator of the transaction repository server, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the blank electronic ballot (*i.e., The digital signature capability is used to authenticate data that is both transmitted and received – col. 36, lines 4-6. This implies a blank electronic ballot is digitally signed {by means of digital signature} using a private key of a public-private key pair {by Digital Signature Standard} prior to transmission*); and
- transmitting a public key of a public-private key pair of the transaction repository server (*inherently included*).

As per **claims 13, 30 and 39**, McClure et al. disclose the method of claims 1, 23 and 35, respectively, wherein the step of transmitting a voted electronic ballot comprises:

- executing the blank electronic ballot (*i.e., Once the voter activates the cast ballot button ... -- col. 37, line 26*);
- encrypting the voted electronic ballot using a symmetric cryptographic function and a symmetric key that is randomly generated by the second computer (*i.e., Once the voter activates the cast ballot button, the executable code stored previously encrypts the resulting/voted data using information from the identification file {which is created with*

data supplied by the Internet software and random information about the voter's computer – col. 36, lines 46-48} ... -- col. 37, lines 26-29);

- encrypting the symmetric key using a public key of a public-private key pair of the transaction repository server (*understood by the public-key encryption standard*); and
- digitally signing the encrypted voted electronic ballot and the encrypted symmetric key using a private key of a public-private key pair, wherein the public-private key pair is generated using an asymmetric cryptographic function, wherein a public key of the public-private key pair is associated with a cryptographic identification of the registered voter, and wherein the public-private key pair and the cryptographic identification are created prior to transmitting the voted electronic ballot (*i.e., The digital signature capability is used to authenticate data that is both transmitted and received – col. 36, lines 4-6. This implies an encrypted voted electronic ballot is digitally signed {by means of digital signature} using a private key of a public-private key pair {by Digital Signature Standard} prior to transmission*).

As per **claim 16**, McClure et al. disclose the method of claim 13, comprising:

- reconciling transmitted voted electronic ballots by an operator of the transaction repository server to establish the validity of each transmitted voted electronic ballot (*i.e., The Internet software, secure behind the firewall, decrypts the transmission and converts the responses of the voter into equivalent switch positions for the voting tablet. After verifying valid switch positions, ... , the Internet software randomly saves the ballot image in a secure database and flags the issue number as no longer valid – col. 37, lines 30-36)*.

As per **claim 17**, McClure et al. disclose the method of claim 16, comprising:

- separating a plurality of valid encrypted voted electronic ballots into groups based on at least one characteristic (*i.e., The interface with the voter during the voting process can occur in any language. The jurisdiction can provide different languages simply by the voter selecting their language of choice at the beginning of the voting process – col. 37, lines*

39-42. This is understood as automatically separating a plurality of valid encrypted voted electronic ballots by languages);

- stripping the digital signature and the cryptographic identification of the registered voter from each group of valid encrypted voted electronic ballots (*i.e., The Internet software, secure behind the firewall, decrypts/strips the transmission {which, as understood, includes the digital signature and the cryptographic identification of the registered voter} and converts the responses of the voter into equivalent switch positions for the voting tablet -- col. 37, lines 30-32)*; and
- randomly mixing within each group the separated encrypted voted electronic ballots (*i.e., After verifying valid switch positions, ... , the Internet software randomly saves the ballot image in a secure database and flags the issue number as no longer valid – col. 37, lines 32-36*).

As per **claim 18**, McClure et al. disclose the method of claim 17, wherein the at least one characteristic is a type of voted electronic ballot (*i.e., The interface with the voter during the voting process can occur in any language. The jurisdiction can provide different languages simply by the voter selecting their language of choice at the beginning of the voting process – col. 37, lines 39-42. This is understood as automatically separating a plurality of valid encrypted voted electronic ballots by languages*).

As per **claims 19, 31 and 40**, McClure et al. disclose the method of claims 17, 30 and 39, respectively, comprising:

- decrypting the encrypted symmetric key of each separated voted electronic ballot using a private key of the public-private key pair of the transaction repository server (*i.e., The Internet software, secure behind the firewall, decrypts/strips the transmission {which, as understood, includes the digital signature and the cryptographic identification of the registered voter, the encrypted key, etc.} and converts the responses of the voter into equivalent switch positions for the voting tablet -- col. 37, lines 30-32)*;

- decrypting the encrypted voted electronic ballot using the symmetric key to recover the voted electronic ballot (*i.e., The Internet software, secure behind the firewall, decrypts/strips the transmission {which, as understood, includes the digital signature and the cryptographic identification of the registered voter, the encrypted key, the encrypted voted electronic ballot itself, etc.} and converts the responses of the voter into equivalent switch positions for the voting tablet. After verifying valid switch positions, as indicated for the voter's ballot style, the Internet software randomly saves the ballot image in a secure database … -- col. 37, lines 30-36)*; and
- printing the voted electronic ballot (*i.e., This data is the sum of all voting tablets 56 and can immediately provide unofficial results for that precinct 48 by use of a precinct printer – col. 44, lines 6-9*).

As per **claims 23 and 32**, McClure et al. disclose a method for completing and submitting an electronic voter registration form and an electronic ballot transmitted over a network, comprising the steps of:

- transmitting a voted electronic ballot from a second computer to the computer database that resides on the transaction repository server (*i.e., Once the voter activates the cast ballot button, the executable code stored previously encrypts the resulting data using information from the identification file and transmits the data packet {i.e., including the voted ballot} to the Internet software host -- col. 37, lines 26-29; After verifying valid switch positions, … , the Internet software randomly saves the ballot image in a secure database … -- col. 37, lines 32-36).*

McClure et al., do not expressly disclose such a method comprising the steps of:

- transmitting a blank electronic registration form, upon request at a first computer, to the first computer; and
- transmitting registration information from a first computer to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter; and

Bayer et al., however, suggest a method for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising the steps of:

- transmitting a blank electronic registration form, upon request at a first computer, to the first computer *(i.e., "**The system** allows voters, or other registrants, to register at one of the registration campaigns at the registration site, which may be linked to a voting campaign, **by constructing a registration questionnaire based on the registration information stored in the database, and sending the questionnaire in a registration form page in the voter's language to the voter** to complete and return to the network server for storage of the voter's registration data" – Abstract: the last sentence, col. 29 line 64 – col. 30 line 8)*;
- transmitting registration information from the first computer, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter (*i.e., "**The system** allows voters, or other registrants, to register at one of the registration campaigns at the registration site, which may be linked to a voting campaign, by constructing a registration questionnaire based on the registration information stored in the database, and sending the questionnaire in a registration form page in the voter's language to the voter **to complete and return to the network server for storage of the voter's registration data**" – Abstract: the last sentence, col. 30 lines 8-13*);

to establish a registered voter over the network/Internet.

Therefore, it would have been obvious to and motivated by an ordinary skill in the art at the time the invention was made to modify a method for completing and submitting an electronic voter registration form and an electronic ballot over a network as disclosed by McClure et al. to include "***transmitting a blank electronic registration form, upon request at a first computer to the first computer; transmitting registration information from the first computer, to a computer database that resides on a transaction repository server, all of which are networked together, to establish a registered voter***" as suggested by Bayer et al. to establish a registered voter over the network.

As per **claim 25**, Bayer et al. disclose the method of claim 23, comprising:

- transmitting a blank electronic registration form, upon request at a first computer, to the first computer *(i.e., "**The system** allows voters, or other registrants, to register at one of the registration campaigns at the registration site, which may be linked to a voting campaign, **by constructing a registration questionnaire based on the registration information stored in the database, and sending the questionnaire in a registration form page in the voter's language to the voter** to complete and return to the network server for storage of the voter's registration data" – Abstract: the last sentence, col. 29 line 64 – col. 30 line 8)*;

As per **claims 26 and 33**, McClure et al. disclose the method of claims 25 and 32, respectively, comprising:

- transmitting a blank electronic ballot, upon request by the registered voter at the second computer, from the computer database that resides on the transaction repository server to the second computer (*i.e., The voter returns to the jurisdiction's home page and selects the cast ballot option – col. 37, lines 4-5; The ballot style information supplied by the issue number allows the Internet voting software to retrieve the ballot style data {i.e., blank electronic ballot} from the database and display it on the screen for the voter – col. 37, lines 17-20*).

As per **claim 35**, McClure et al. disclose the method of claim 33, comprising:

- transmitting a voted electronic ballot from the second computer to the computer database that resides on the transaction repository server (*i.e., Once the voter activates the cast ballot button, the executable code stored previously encrypts the resulting data using information from the identification file and transmits the data packet {i.e., including the voted ballot} to the Internet software host -- col. 37, lines 26-29; After verifying valid switch positions, ... , the Internet software randomly saves the ballot image in a secure database ... -- col. 37, lines 32-36*).

Claim Rejections - 35 USC §102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. §102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.*

Claims 20-22, 41-47 are rejected under 35 U.S.C. §102(e) as being anticipated by McClure et al., U.S. Patent No. 6,250,548 B1, published 26 June 2001.

As per **claim 20**, McClure et al. disclose a method for verifying at least one of a voter registration status and an electronic ballot status in a voting system, comprising the steps of:

- establishing at least one computer database on a transaction repository server that contains information associated with at least one of the voter registration status of a citizen and the electronic ballot status (i.e., *the voter registration database – col. 9, lines 29-33, the tallying and reports databases – col. 9, lines 47-49, all of which, of course, reside on servers*);
- receiving, from a first computer connected to a computer network, a citizen's request regarding status of at least one of the citizen's voter registration and the citizen's electronic ballot status (*i.e., "Once registered, the voter submits a request to vote" – col. 36 lines 30-33. By doing this, the voter implicitly & inherently initiates a request for a status of his/her voting registration/eligibility, which is then determined/verified/approved with the assignment of an Issue number {see col. 33 lines 22-47 for more info.} for the voter to be able to cast one and only one ballot – col. 36 lines 59-67. The voting registration/eligibility is further shown in "The voter returns to the jurisdiction's home page, selects the cast ballot option ... Given a valid issue no., the id file is verified as*

***legitimate/eligible/legal/valid**, and the voter gains access to the cast ballot selection" – col. 37 lines 4-15, col. 42 lines 36-50*);

- determining a status message in response to the step of receiving by examining the at least one computer database (*i.e., Electronic officials verify the information supplied by the voter and approve the assignment of an "issue number" for the voter – col. 36, lines 59-61*); and
- transmitting the status message from the transaction repository server to the first computer over the computer network (*i.e., The issue number {understood as the status} is electronically sent to the voter via the Internet to the address supplied by the voter and defines the proper ballot style for the voter – col. 36, lines 61-63*).

As per **claim 21**, McClure et al. disclose the method of claim 20, wherein a transaction mediator communicates information between the first computer and the transaction repository server (*i.e., as understood, the Internet voting software/browser {as a transaction mediator} transmits and receives {communicates} information between the voter's computer and the Internet voting software host/server*).

As per **claim 41**, McClure et al. disclose a system for completing and submitting an electronic voter registration form and an electronic ballot over a network, comprising:

- a transaction repository server for transmitting a blank electronic ballot to a first computer (*i.e., the Internet voting software host/server, on which the Internet voting software resides, allows the software to retrieve the ballot style data {understood as a blank electronic ballot} from the database and display it on the screen for the voter – col. 37, lines 18-20*);
- a computer database, accessible by the transaction repository server, for storing the blank electronic ballot (*i.e., the Internet voting software host/server, on which the Internet voting software resides, allows the software to retrieve the ballot style data {understood as a blank electronic ballot} from the database and display it on the screen for the voter – col. 37, lines 18-20*); and

- a transaction mediator for communicating information between the transaction repository server and the first computer, the transaction mediator being operative to transmit registration information from the first computer to the computer database to establish a registered voter (*i.e., the Internet voting software such as browsers – col. 36, lines 30-35*).

As per **claim 42**, McClure et al. disclose the system of claim 41, wherein the transaction mediator is operative to transmit the voted electronic ballot from the first computer to the computer database (*i.e., the Internet voting software such as browsers transmits the data packet {which includes encrypted voted electronic ballot} to the Internet software host/server – col. 37, lines 26-29*).

As per **claim 43**, McClure et al. disclose the system of claim 42, wherein the first computer comprises multiple computers (i.e., The subsystem 46 at each of the precincts 48 includes ... a network of voting stations/computers 52, ... -- col. 7, lines 41-44).

As per **claim 46**, McClure et al. disclose a system for verifying at least one of a voter registration status and all electronic ballot status in a voting system, comprising:

- a first computer connected to a computer network by which a citizen can request at least one of the citizen's voter registration status and the citizen's electronic ballot status from a transaction repository server (*i.e., "Once registered, the voter submits a request to vote" – col. 36 lines 30-33. By doing this, the voter implicitly & inherently initiates a request for a status of his/her voting registration/eligibility, which is then determined/verified/approved with the assignment of an Issue number {see col. 33 lines 22-47 for more info.} for the voter to be able to cast one and only one ballot – col. 36 lines 59-67. The voting registration/eligibility is further shown in "The voter returns to the jurisdiction's home page, selects the cast ballot option ... Given a valid issue no., the id file is verified as **legitimate/eligible/legal/valid**, and the voter gains access to the cast ballot selection" – col. 37 lines 4-15, col. 42 lines 36-50*); and
- at least one computer database, accessible by the transaction repository server, for containing information associated with at least one of the voter registration status of a

citizen and the electronic ballot status (i.e., *the voter registration database – col. 9, lines 29-33, the tallying and reports databases – col. 9, lines 47-49, all of which, of course, accessible by the Internet voting software host/server*);

- the transaction repository server being operative for determining a status message in response to the status request by examining the at least one computer database, and for transmitting the status message to the first computer (*i.e., the Internet voting software host/server – col. 37, line 29*).

Conclusion

Examiner has cited particular columns and line numbers and/or paragraph and/or page numbers in the prior arts of record as applied to the claims above in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to fully consider the references in its **entirety** as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the examiner should be directed to NANCY LOAN T. LE

whose telephone number is **(571) 272-7066**. The examiner can normally be reached on Monday - Friday, 9am - 6:00pm Eastern Standard Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, ANDREW J. FISCHER can be reached on **(571) 272-6779**.

For **official/regular communication**, the fax number for the organization where this application or proceeding is assigned is **(571) 273-8300**.

For **informal/draft communication**, the fax number is **(571) 273-7066 (Rightfax)**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see **http://pair-direct.uspto.gov**. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866-217-9197 (toll-free).**

Nancy Le

Patent Examiner

15 October 2007

CALVIN L. HEWITT II
PRIMARY EXAMINER